Cisco FIPS Object Module

Firmware Version: 7.2

FIPS 140-2 Non-Proprietary Security Policy
Level 1 Validation

Version 1.0

January 4, 2021

Table of Contents

1 INTRODUCTION 1

1.1 PURPOSE 1
1.2 MODULE VALIDATION LEVEL 1
1.3 REFERENCES 2
1.4 TERMINOLOGY 2
1.5 DOCUMENT ORGANIZATION 2

2 CISCO FIPS OBJECT MODULE 3

2.1 MODULE INTERFACES 4
2.2 ROLES AND SERVICES 6
2.2.1 Crypto-Officer Role 6
2.2.2 User Role 6
2.3 PHYSICAL SECURITY 7
2.4 CRYPTOGRAPHIC ALGORITHMS 8
2.4.1 Approved Cryptographic Algorithms 8
2.4.2 Non-FIPS Approved Algorithms Allowed in FIPS mode 9
2.5 CRYPTOGRAPHIC KEY MANAGEMENT 9
2.5.1 Key Generation 10
2.5.2 Key Storage 10
2.5.3 Key Access 10
2.5.4 Key Protection and Zeroization 10
2.6 SELF-TESTS 12

3 SECURE DISTRIBUTION, OPERATION, AND USER GUIDANCE 14

3.1 SECURE DISTRIBUTION 14
3.2 SECURE INITIALIZATION 14
3.3 SECURE OPERATION 14
3.4 USER GUIDANCE 15
3.4.1 Triple-DES Keys 15
3.4.2 AES GCM IV Generation 15

APPENDIX A – ACRONYMS AND ABBREVIATIONS 16

1 Introduction

1.1 Purpose

This document is the non-proprietary Cryptographic Module Security Policy for the Cisco FIPS Object Module (FOM). This security policy describes how the FOM (Firmware Version: 7.2) meets the security requirements of FIPS 140-2, and how to operate it in a secure FIPS 140-2 mode. This policy was prepared as part of the Level 1 FIPS 140-2 validation of the Cisco FIPS Object Module.

FIPS 140-2 (Federal Information Processing Standards Publication 140-2 — *Security Requirements for Cryptographic Modules*) details the U.S. Government requirements for cryptographic Modules. More information about the FIPS 140-2 standard and validation program is available on the NIST website at http://csrc.nist.gov/groups/STM/index.html.

1.2 Module Validation Level

The following table lists the level of validation for each area in the FIPS PUB 140-2.

Table 1 - Module Validation Level

No.	Area Title	Level
1	Cryptographic Module Specification	1
2	Cryptographic Module Ports and Interfaces	1
3	Roles, Services, and Authentication	1
4	Finite State Model	1
5	Physical Security	1
6	Operational Environment	N/A
7	Cryptographic Key management	1
8	Electromagnetic Interface/Electromagnetic Compatibility	1
9	Self-Tests	1
10	Design Assurance	3
11	Mitigation of Other Attacks	N/A
	Overall Module validation level	**1**

1.3 References

This document deals only with operations and capabilities of the Cisco FIPS Object Module in the technical terms of a FIPS 140-2 cryptographic Module security policy. More information is available from the following sources:

For answers to technical or sales related questions please refer to the contacts listed on the Cisco Systems website at www.cisco.com.

The NIST Validated Modules website (http://csrc.nist.gov/groups/STM/cmvp/validation.html) contains contact information for answers to technical or sales-related questions for the module.

1.4 Terminology

In this document, the Cisco FIPS Object Module (FOM) is referred to as FOM, the cryptographic module or the module.

1.5 Document Organization

The Security Policy document is part of the FIPS 140-2 Submission Package. In addition to this document, the Submission Package contains:

- Vendor Evidence document
- Finite State Machine
- Other supporting documentation as additional references

This document provides an overview of the Cisco FIPS Object Module and explains the secure configuration and operation of the module. This introduction section is followed by Section 2, which details the general features and functionality of the module. Section 3 specifically addresses the required configuration for the FIPS-mode of operation.

With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 Validation Submission Documentation is Cisco-proprietary and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact Cisco Systems.

2 Cisco FIPS Object Module

The Cisco FIPS Object Module (FOM) is a firmware library that provides cryptographic services to a vast array of Cisco's networking and collaboration products. The Cisco product lines that include FOM to provide FIPS 140-2 validated cryptographic functionalities are as below:

Cisco Catalyst IoT, LAN and Enterprise Switches including Wireless Controllers and Access Points
Cisco WAN Aggregation and Internet Edge Routers
Cisco Nexus Data Center Switches
Cisco SD-WAN Viptela Solutions
Cisco Firewalls
Cisco Telepresence and Communication Systems

The cryptographic module provides primitives of secure protocols such as IKEv2/IPSec, sRTP, SSH, TLS, and SNMPv3. It does not implement any of these security protocols, instead it provides the cipher operation and Key Derivative Function (KDF) functionalities for the services.

The module is based on the OpenSSL FIPS canister with additions to support Suite B algorithms. For the purposes of FIPS 140-2 level 1 validation, the FOM is a single object module file named fipscanister.o (Linux / FreeBSD Android) or fipscanister.lib (Microsoft Windows). The object code in the object module file is incorporated into the runtime executable application at the time the binary executable is generated. The module performs no communications other than with the consuming application (the process that invokes the module services via the module's API), which can be considered as the host for the module.

The module's logical block diagram is shown in Figure 1 below.

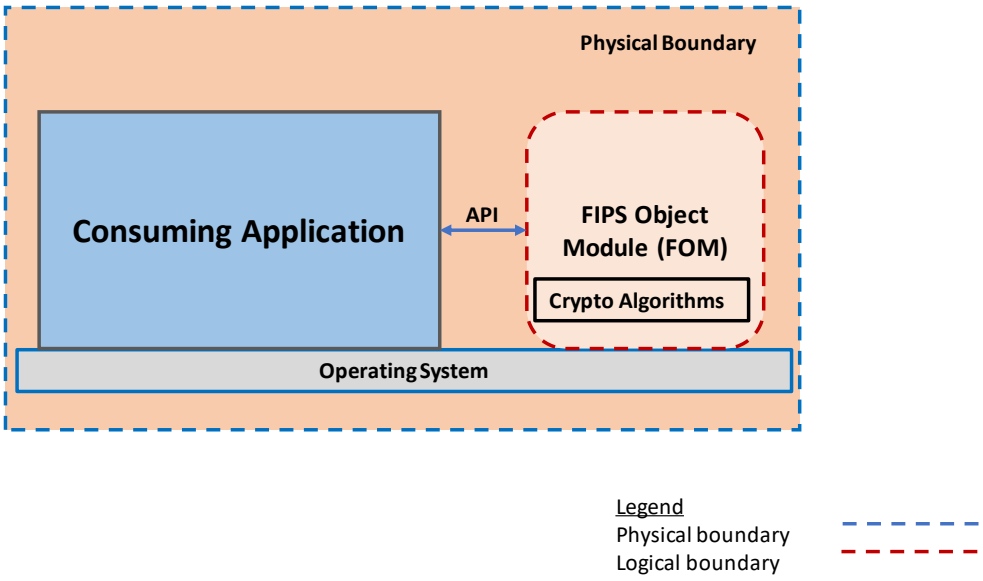

Figure 1 – Cisco FIPS Object Module Block Diagram Depicting Cryptographic Boundary

The dashed red border denotes the logical cryptographic boundary of the module. The physical cryptographic boundary of the module is the enclosure of the system on which it is executing and is denoted by the dashed blue border.

This module was tested on the following platforms for the purposes of this FIPS 140-2 validation:

Table 2 - Tested Operational Environments (OEs)

#	Platform	Processor	Operating Systems	ACVP Certificate
1	Evaluation board	Cavium Octeon CN5230	Linux 2.6	A110
2	Cisco Catalyst 9300	Intel Xeon D-1526 (with AES-NI)	Linux 4.4	A114
3	Cisco Catalyst 9200	ARM 8 Cortex-A53 AArch64	Linux 4.4	A109
4	Cisco UCS M5	Intel Xeon Gold 6128 (with AES-NI)	Linux 4.18	A112
5	Cisco ASA 5555	Intel Xeon X3460	Linux 4.1	A111
6	Cisco Nexus 3172	Intel Pentium B 925C (with AES-NI)	Linux 4.1	A105
7	Cisco ISR 4451	Intel Xeon E3-1105C (with AES-NI)	Linux 4.4	A106
8	Cisco Firepower 9300	Intel Xeon E5-2658 (with AES-NI)	Linux 4.1	A113
9	Cisco ISR 4351	Intel Atom C2758 (with AES-NI)	Linux 4.4	A108

2.1 Module Interfaces

The physical ports of the module are the same as the system on which it is executing. The logical interface is a C-language application program interface (API).

The Data Input interface consists of the input parameters of the API functions. The Data Output interface consists of the output parameters of the API functions. The Control Input interface consists of the actual API functions. The Status Output interface includes the return values of the API functions.

The module provides a number of physical and logical interfaces to the application (and the device upon which it is running), and the physical interfaces provided by the module are mapped to the following FIPS 140-2 defined logical interfaces: data input, data output, control input, and status output. The logical interfaces and their mapping are described in the following table:

Table 3 - FIPS 140-2 Logical Interfaces

Interface	Description
Data Input	API input parameters - plaintext and/or ciphertext data
Data Output	API output parameters - plaintext and/or ciphertext data
Control Input	API function calls - function calls, or input arguments that specify commands and control data used to control the operation of the module
Status Output	API return codes- function return codes, error codes, or output arguments that receive status information used to indicate the status of the module
Power	Not Applicable

2.2 Roles and Services

The module meets all FIPS 140-2 level 1 requirements for Roles and Services, implementing both User and Crypto-Officer roles. The module does not authenticate the roles. Only one role may be active at a time.

2.2.1 Crypto-Officer Role

Crypto-Officer (CO) role is responsible for installing the module on the host computer system. The CO role is implicitly entered during installation process or performing system administration functions on the host operating system.

The following table lists the approved or non-approved but allowed services available in FIPS 140-2 approved mode. The services available to the CO role accessing the Critical Security Parameters (CSPs), the type of access – read (r), write (w), execute (e) and zeroized/delete (d) – and which role accesses the CSPs are listed below:

Table 4 - Roles, Services, and Keys in FIPS 140-2 Approved Mode of Operation

Service	CSP	Access
Module Installation	None	N/A
Show status	None	N/A
Module initialization	None	N/A
Perform Self-test	None	N/A
Uninstallation	All CSPs	d

2.2.2 User Role

User role has access to all of the cryptographic services provided by the module. The following table lists the approved or non-approved but allowed services available in FIPS 140-2 approved mode. The services available to the User role accessing the CSPs, the type of access – read (r), write (w), execute (e) and zeroized/delete (d) – and which role accesses the CSPs are listed below:

Table 5 - User Role Services Available in FIPS Mode of Operation

Service	CSP	Access
Symmetric encryption/decryption	Symmetric Keys	r, w, e, d
Symmetric Legacy Decryption	Symmetric Legacy Key	r, w, e, d
Symmetric Digest	Symmetric Keys	r, w, e, d
AES Key Wrap (KW)	Symmetric Keys (NIST SP 800-38F AES Key Wrapping using both KW mode with 128/192/256-bit AES key)	r, w, e, d
Asymmetric Encryption and Decryption	Asymmetric Keys	r, w, e, d
Digital signature generation and verification	Asymmetric Keys	r, w, e, d
Asymmetric Key Generation	Asymmetric Keys	r, w, e, d
Symmetric Key Generation	Symmetric Keys	r, w, e, d
Key exchange component	Diffie-Hellman/EC Diffie-Hellman key components	r, w, e, d
Key establishment component	Key agreement scheme components	r, w, e, d
Key Derivation Function (KDF)	KDF Keys	r, w, e, d
Keyed Hash (HMAC)	Keyed Hash key	r, w, e, d
Message digest (SHS)	None	-
Random number generation	DRBG Input	r, w, e, d
Zeroization	All CSPs	d

2.3 Physical Security

Per FIPS 140-2 classification, this is a multi-chip standalone cryptographic module. FOM 7.2 is a firmware only module and runs on production grade chassis.

2.4 Cryptographic Algorithms

The module supports the following FIPS 140-2 approved algorithm implementations:

2.4.1 Approved Cryptographic Algorithms

Table 6 - Approved Cryptographic Algorithms

Algorithm	Algorithm Capabilities	Algorithm Certificate Numbers
AES	Key sizes: 128, 192, 256 bits Modes: CBC, CCM, CFB1/8/128, CMAC, CTR, ECB, GCM, GMAC, KW, OFB, XTS[1]	A105, A106, A108, A109, A110, A111, A112, A113, A114
SP800-90A DRBG	HASH_DRBG, HMAC_DRBG, CTR_DRBG	
DSA	Key sizes: 2048, 3072 bits KeyGen, PQGGen, PQGVer, SigGen, SigVer	
ECDSA	Curves: P-224, P-256, P-384, P-521, K-233, K-283, K-409, K-571, B-233, B-283, B-409, B-571 KeyGen, KeyVer, SigGen, SigVer	
HMAC	HMAC-SHA-1, HMAC-SHA2-224, HMAC-SHA2-256, HMAC-SHA2-384, HMAC-SHA2-512, HMAC-SHA2-512/224, HMAC-SHA2-512/256, HMAC-SHA3-224, HMAC-SHA3-256, HMAC-SHA3-384, HMAC-SHA3-512	
CVL (SP800-56A)	KAS-ECC CDH-Component: Curves: B-233, B-283, B-409, B-571, K-233, K-283, K-409, K-571, P-224, P-256, P-384, P-521 KAS-ECC Component: Curves: P-224, P-256, P-384, P521 KAS-FFC Component: FB: SHA2-224, SHA2-256 FC: SHA2-256	
CVL (SP800-135)[2]	SNMPv3, sRTP, TLS, SSHv2, IKEv2	

[1] AES-XTS: 128-bit and 256-bit only

[2] There is no other part of protocols (IKEv2, TLS, SSH, sRTP and SNMPv3), except the KDF, have been reviewed or tested by the CAVP and CMVP. Please refer IG D.11, bullet 2 for more information.

Algorithm	Algorithm Capabilities	Algorithm Certificate Numbers
KBKDF (SP800-108)	Mode: Counter MAC Mode: HMAC-SHA-1, HMAC-SHA2-224, HMAC-SHA2-256, HMAC-SHA2-384, HMAC-SHA2-512	
RSA	Key sizes: 2048, 3072, 4096 bits KeyGen, SigGen, SigVer,	
SHS	SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512	
SHA-3	SHA3-224, SHA3-256, SHA3-384, SHA3-512	
Triple-DES	Keying option: 1 Modes: CBC, CFB1/CFB8/CFB64, CMAC, CTR, ECB, OFB	
CKG (SP800-133)[3]		Vendor Affirmed

2.4.2 Non-FIPS Approved Algorithms Allowed in FIPS mode

The module supports the following non-FIPS approved algorithms which are permitted for use in the FIPS approved mode:[4]

- Diffie-Hellman (CVL Certs. #A105, #A106, #A108, #A109, #A110, #A111, #A112, #A113 and #A114, key agreement; key establishment methodology provides between 112 and 219 bits of encryption strength)
- EC Diffie-Hellman (CVL Certs. #A105, #A106, #A108, #A109, #A110, #A111, #A112, #A113 and #A114, key agreement; key establishment methodology provides between 112 and 256 bits of encryption strength)
- RSA (key wrapping; key establishment methodology provides between 112 and 132 bits of encryption strength)

2.5 Cryptographic Key Management

Cisco FIPS Object Module operates only in FIPS mode of operation. The module implements a variety of approved algorithms. This section describes life cycle of a Critical Security Parameter (CSP) that includes key generation/entry methods, storage, output and zeroization process.

[3] CKG (vendor affirmed) Cryptographic Key Generation; In accordance with FIPS 140-2 IG D.12, the cryptographic module performs Cryptographic Key Generation as per scenario 1 of section 4 in SP800-133rev1. The resulting generated symmetric key and the seed used in the asymmetric key generation are the unmodified output from SP800-90A DRBG

[4] See IG 7.5 for an explanation of the basis of ranges of bit strength caveats

2.5.1 Key Generation

The module supports generation of DH, ECDH, FIPS 186-4 DSA, FIPS 186-4 RSA, and FIPS 186-4 ECDSA public-private key pairs. The module employs a NIST SP 800-90A random number generator for creation of both symmetric keys and the seed for asymmetric key generation.

The entropy and seeding material for the NDRNG is provided to it by the external calling application (and not by the module) which is outside the module's logical boundary but contained within the module's physical boundary. The minimum effective strength of the SP 800-90A DRBG seed is required to be at least 112 bits when used in a FIPS approved mode of operation, therefore the minimum number of bits of entropy requested when the module makes a call to the SP 800-90A DRBG is 112. No assurance of the minimum strength of generated keys.

The module users (the external calling applications) shall use entropy sources which meet the security strength required for the random number generation mechanism as shown in SP 800-90A based on Hash_DRBG, HMAC_DRBG, and CTR_DRBG. This entropy is supplied by means of callback functions. Those functions must return an error if the minimum entropy strength cannot be met.

2.5.2 Key Storage

Public and private keys are provided to the module by the calling process and are destroyed when released by the appropriate API function calls. The module does not perform persistent storage of keys.

2.5.3 Key Access

An authorized application as user (the Crypto-User) has access to all key data generated during the operation of the module.

2.5.4 Key Protection and Zeroization

Keys residing in internally allocated data structures can only be accessed using the module defined API. The operating system protects memory and process space from unauthorized access. Zeroization of sensitive data is performed automatically by API function calls for intermediate data items.

Only the process that creates or imports keys can use or export them. No persistent storage of key data is performed by the module. All API functions are executed by the invoking process in a non-overlapping sequence such that no two API functions will execute concurrently.

All CSPs can be zeroized by power-cycling the module (with the exception of the firmware Integrity key). In the event module power is lost and restored the consuming application must ensure that any AES-GCM keys used for encryption or decryption are re-distributed.

The module supports the following FIPS 140-2 approved keys and Critical Security Parameters (CSPs):

Table 7 - Cryptographic Keys and CSPs

ID	Algorithm	Description
Asymmetric Keys	RSA: Key sizes: 2048, 3072, 4096 bits DSA: Key sizes: 2048, 3072 bits ECDSA: Curves: P-224, P-256, P-384, P-521, K-233, K-283, K-409, K-571, B-233, B-283, B-409, B-571	Used for signature generation and verification. RSA: Also used for encryption and decryption
Symmetric Keys	AES: Key sizes: 128, 192, 256 bits Modes: CBC, CCM, CFB1/8/128, CMAC, CTR, ECB, GCM, GMAC, KW, OFB, XTS TDES: Keying option: 1 Modes: CBC, CFB1/CFB8/CFB64, CMAC, CTR, ECB, OFB	Used for symmetric encryption and decryption, MAC, and key wrap
Diffie-Hellman/EC Diffie-Hellman key components	DH: Public Key – 2048-10,000 bits Private Key – 224-512 bits ECDH: P-224, P-256, P-384, P-521, K-233, K-283, K-409, K-571, B-233, B-283, B-409, B-571	Used for key agreement scheme
Key agreement scheme components	KAS-ECC CDH-Component: Curves: B-233, B-283, B-409, B-571, K-233, K-283, K-409, K-571, P-224, P-256, P-384, P-521 KAS-ECC Component: Curves: P-224, P-256, P-384, P521 KAS-FFC Component: FB: SHA2-224, SHA2-256 FC: SHA2-256	A key establishment scheme may use these components
DRBG Input	HASH_DRBG: length dependent on security strength HMAC_DRBG: length dependent on security strength CTR_DRBG: length dependent on security strength	DRBG implementations per NIST SP 800-90A.
DRBG Internal States	HASH_DRBG: V(440/888 bits) C(440/888 bits)	DRBG implementations per NIST SP 800-90A.

ID	Algorithm	Description
	HMAC_DRBG: V (160/224/256/384/512 bits) Key (160/224/256/384/512 bits)	
	CTR_DRBG: V (128 bits) Key (AES 128/192/256)	
Keyed Hash key	All supported key sizes for HMAC: HMAC-SHA-1, HMAC-SHA2-224, HMAC-SHA2-256, HMAC-SHA2-384, HMAC-SHA2-512, HMAC-SHA2-512/224, HMAC-SHA2-512/256, HMAC-SHA3-224, HMAC-SHA3-256, HMAC-SHA3-384, HMAC-SHA3-512 (Key sizes must be a minimum of 112-bits)	Used for keyed hash
Firmware Integrity key	HMAC-SHA-1	Used to perform firmware integrity test at power-on. This key is embedded within the module.
Key Derivation Function (KDF) Keys	SNMPv3 Session Key: AES (128-bits)	Derived via key derivation function defined in SP800-135 KDF (SNMPv3).
	SRTP Key: AES (128-, 192-, 256-bits)	Derived via key derivation function defined in SP800-135 KDF (SRTP).
	TLS Master Secret: 48 bytes of shared secret (DRBG data)	Derived via key derivation function defined in SP800-135 KDF (TLS).
	SSHv2 Session Key: AES (128-, 192-, 256-bits)	Derived via key derivation function defined in SP800-135 KDF (SSH).
	SKEYSEED: 20 bytes of shared secret	Derived via key derivation function defined in SP800-135 KDF (IKEv2).
	SKEYID: 20 bytes of shared secret	Derived via key derivation function defined in SP800-135 KDF (IKEv2).
	IKEv2 session authentication key: HMAC-SHA-1	Derived via key derivation function defined in SP800-135 KDF (IKEv2).
	IKEv2 session encryption key: AES (128-, 192-, 256-bits)	Derived via key derivation function defined in SP800-135 KDF (IKEv2).

2.6 Self-Tests

The module performs both Power-On Self-Tests (POSTs) at the module initialization and continuous conditional tests during operation. Input, output, and cryptographic functions cannot be performed while the module is in a self-test or error state as the module is single threaded and will not return to the calling application until the POSTs are

complete. If the POSTs fail subsequent calls to the module will fail and thus no further cryptographic operations are possible.

Power-On Self-Tests (POST) Performed

- AES Known Answer Test (Separate encrypt and decrypt)
- AES-CCM Known Answer Test (Separate encrypt and decrypt)
- AES-GCM Known Answer Test (Separate encrypt and decrypt)
- AES-CMAC Known Answer Test
- AES-XTS Known Answer Test (Separate encrypt and decrypt)
- SP 800-90A DRBG Known Answer Tests
    - HASH_DRBG Known Answer Test
    - HMAC_DRBG Known Answer Test
    - CTR_DRBG Known Answer Test
- FIPS 186-4 DSA Sign/Verify Test (2048, SHA-384)
- FIPS 186-4 ECDSA Sign/Verify Test (P-256, SHA-512)
- HMAC Known Answer Tests
    - HMAC-SHA1 Known Answer Test
    - HMAC-SHA224 Known Answer Test
    - HMAC-SHA256 Known Answer Test
    - HMAC-SHA384 Known Answer Test
    - HMAC-SHA512 Known Answer Test
- ECC CDH KAT
- FIPS 186-4 RSA Known Answer Test (Separate sign and verify. 2048, SHA-256)
- SHA-1 Known Answer Test
- SHA-3 (256, 512) Known Answer Test
- Firmware Integrity Test (HMAC-SHA1)
- Triple-DES Known Answer Test (Separate encrypt and decrypt)
- Triple-DES CMAC Known Answer Test (Separate encrypt and decrypt)
- KBKDF Known Answer Test

Conditional tests

- Pairwise consistency tests for RSA, DSA, and ECDSA
- SP 800-90A DRBG Continuous random number generation tests
    - HASH_DRBG Continuous random number generation test
    - HMAC_DRBG Continuous random number generation test
    - CTR_DRBG Continuous random number generation test

Critical Function Tests (applicable to the DRBG, as per SP 800-90A, Section 11)

- Instantiate Test
- Generate Test
- Reseed Test
- Uninstantiate Test

FIPS mode of operation can only be enabled after the consuming application invokes the *FIPS_mode_set()*. The function checks that the initialization sequence and the aforementioned POSTs have completed successfully.

3 Secure Distribution, Operation, and User Guidance

3.1 Secure Distribution

The Cisco FOM is distributed only for use by Cisco personnel and as such is accessible only from the secure Cisco internal repository. Only authorized Cisco personnel have access to the module. The SHA512 fingerprint of the validated distribution tarball file is:

3380374bc4ba51fe951656bf9f015ecfd8fd2d82c9303bd583a5d437d9a2516d5292f9af1b57ce2284e424e5
c6a79394904b83616e9896a20e8861f281c269ab

A complete revision history of the source code from which the module was generated is maintained in a version control database[5].

3.2 Secure Initialization

The Operating System loads the module into its user space. The initialization sequence starts with a check of the integrity of the runtime executable using a HMAC-SHA1 digest computed at build time. If this computed HMAC-SHA1 digest matches the stored known digest then the POSTs, consisting of the algorithm specific Pairwise Consistency and Known Answer tests, are performed. If any component of the Power-On Self-Test fails an internal global error flag is set to prevent subsequent invocation of any cryptographic function calls. Any such POST failure is a hard error that can only be recovered by reinstalling the module. If all components of the self-tests are successful.

Upon loading the cryptographic module, the consuming application enables FIPS mode of operation by calling *FIPS_mode_set()* function. This function call verifies POST outcome and returns a "1" for success and "0" for failure; interpretation of this return code is the responsibility of the host application.

The module is installed using one of the sets of instructions in the 'README.Cisco' document appropriate to the target system available in the repository with the source code.

3.3 Secure Operation

The tested operating systems segregate user processes into separate process spaces. Each process space is an independent virtual memory area that is logically separated from all other processes by the operating system software and hardware. The module functions entirely within the process space of the process that invokes it, and

[5] This database is internal to Cisco since the intended use of this cryptographic module is by Cisco development teams.

thus the module runs on a single user mode of operation. Cisco FIPS Object Module operates only in FIPS mode of operation. There is no non-FIPS mode of operation for the module.

3.4 User Guidance

3.4.1 Triple-DES Keys

In accordance with CMVP IG A.13, when operating in a FIPS approved mode of operation, the same Triple-DES key shall not be used to encrypt more than 2^{20} 64-bit data blocks.

Each of the TLS and SSH protocols governs the generation of the respective Triple-DES keys. Please refer to IETF RFC 5246 (TLS) and IETF RFC 4253 (SSH) for details relevant to the generation of the individual Triple-DES encryption keys. The user is responsible for ensuring that the module limits the number of encrypted blocks with the same key to no more than 2^{20} when utilized as part of a recognized IETF protocol.

For all other uses of Triple-DES the user is responsible for ensuring that the module limits the number of encrypted blocks with the same key to no more than 2^{16}.

3.4.2 AES GCM IV Generation

In the case of AES-GCM, the IV generation method is user-selectable and the value can be computed in more than one manner as follows:

1) **TLS 1.2:** The module's AES-GCM implementation conforms to IG A.5, scenario #1, following RFC 5288 for TLS. The counter portion of the IV is set by the module within its cryptographic boundary. When the IV exhausts the maximum number of possible values for a given session key, the first party, client or server, to encounter this condition will trigger a handshake to establish a new encryption key in accordance with RFC 5246.
2) **Non-TLS 1.2:** The module's AES-GCM implementation conforms to IG A.5, scenario #3, when operating in a FIPS approved mode of operation, AES GCM, IVs are generated both internally and deterministically and are a minimum of 96-bits in length as specified in SP 800-38D, Section 8.2.1.

The selection of the IV construction method is the responsibility of the user of this cryptographic module.

Appendix A – Acronyms and Abbreviations

Term	Expansion / Definition
AES	Advanced Encryption Standard
API	Application Program Interface
CBC	Cipher Block Chaining
CCM	Counter with Cipher Block Chaining-Message Authentication Code
CDH	Cofactor Diffie-Hellman
CFB	Cipher Feedback
CKG	Cryptographic Key Generation (See NIST SP 800-133)
CMAC	Cipher-Based Message Authentication Code
CMVP	Cryptographic Module Validation Program
CO	Crypto-Officer
CSP	Critical Security Parameter
CTR	Counter
CVL	Component Validation List
DES	Data Encryption Standard
DH	Diffie-Hellman
DRBG	Deterministic Random Bit Generator
DSA	Digital Signature Algorithm
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
FIPS	Federal Information Processing Standard
FOM	FIPS Object Module
GCM	Galois/Counter Mode
GMAC	AES Galios Message Authentication Code
HMAC	Hash Message Authentication Code

Term	Expansion / Definition
IKE	Internet Key Exchange
IoT	Internet of Things
IV	Initial Vector
IPSec	Internet Protocol Security
KAT	Known Answer Test
KBKDF	Key Based Key Derivation Function
KDF	Key Derivation Function
KW	Key Wrap
LAN	Local Area Network
MAC	Message Authentication Code
NDRNG	Non-deterministic RNG
NIST	National Institute of Standards and Technology
OFB	Output Feedback
OS	Operating System
POST	Power-On Self-Test
RSA	Rivest Shamir and Adleman
SD-WAN	Software Defined WAN
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
SNMP	Simple Network Management Protocol
SP	Special Publication
sRTP	Secure Real-time Transport Protocol
SSH	Secure Shell
UCS	Unified Computing System
TLS	Transport Layer Security
WAN	Wide Area Network

Term	Expansion / Definition
XOR	Exclusive OR
XTS	XEX Tweakable Block Cipher with Ciphertext Stealing